New Jersey Cybersecurity & Communications Integration Cell

Cybersecurity Strategic Plan 2021-2025

NEW JERSEY CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

A Division of the New Jersey Office of Homeland Security & Preparedness

VISION STATEMENT

A safe, secure, and resilient New Jersey that is able to fully realize the opportunities and benefits of technological innovations that act as an engine for economic growth and societal gains.

MISSION STATEMENT

To lead and coordinate New Jersey's cybersecurity efforts while building resiliency to cyber threats throughout the State.

CORE VALUES

SERVICE. We put our State and its citizens first, and we put Mission before self. We take pride in being timely, agile, and relevant.

TEAMWORK. We stand with and behind each other. We recognize that partnerships, both internal and external, are critical to achieving success. We cannot fulfill our Mission alone.

EXCELLENCE. We take great pride in the quality of our work. We do every task, every project, every initiative, to the best of our ability.

DIVERSITY. We strive to build a workforce that is as diverse as New Jersey's citizenry. We pride ourselves on encouraging diversity of thought, perspective, and problem solving.

INTEGRITY. We are committed to holding ourselves accountable to the highest moral and ethical standards in our personal and professional conduct. We can be relied upon to act with honor and truthfulness.

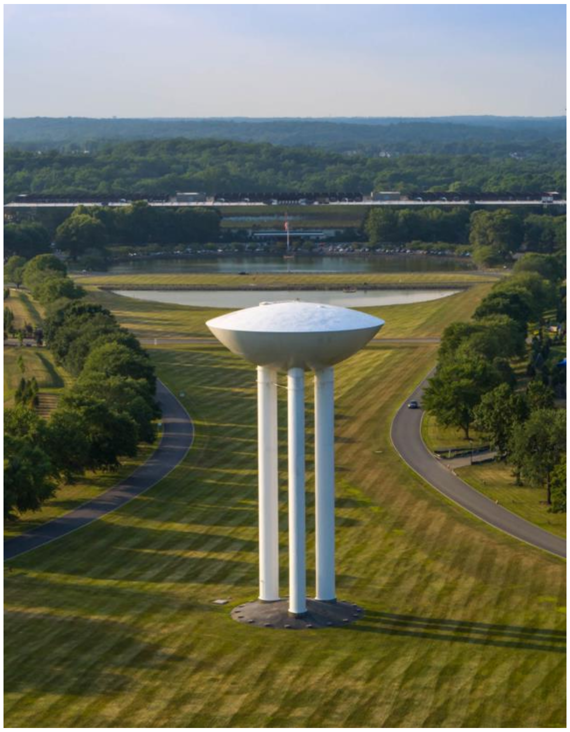
TABLE OF CONTENTS

INTRODUCTION

The development of transistor technology at New Jersey's Bell Labs over 70 years ago ushered in the information age that has transformed the global economy, revolutionized public and private sector institutions, created entirely new industries, and transformed all facets of work, life, and play. At the information age's outset, computers were considered systems of record that helped humans process and store information. Over time, increases in computing power, information storage, and communications enabled computers to evolve from systems of record, to systems of engagement, and now, to systems of interaction. Today, computers are embedded into virtually all physical objects that connect, share, and interact with one another, blurring the lines between the physical and cyber worlds. A new car, for example, has upwards of 50 embedded computers that monitor, control, and communicate with everything from its engine to its safety and entertainment systems, as well as surrounding vehicles and other external systems and devices. Beyond automobiles, connected computers are used to enable and control almost all aspects of business and manufacturing, government services, health care, education, communications, lifeline critical infrastructure, and modern conveniences.

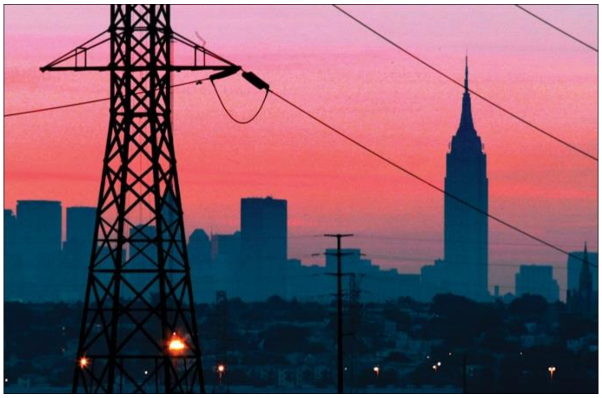
The increasing pace of change and rapid technological advances in areas such as elastic cloud computing, artificial intelligence, autonomous systems, big data, and the Internet of Things (IoT) enables modern society to address classes of applications that were inconceivable just a few years ago, while also creating an Internet of Everything (IoE) comprised of physical and virtual objects, people, processes, and data. This digital transformation and our growing dependence on the confluence of technologies is expected to continue unabated for the foreseeable future, creating an expanding attack surface that provides opportunities for nation states, terrorist organizations, political activists, and criminals to maliciously target cyber infrastructure and information for foreign policy/national interests, financial gain, to foment chaos and anarchy, to sow social division, and for other nefarious motivations.

As New Jersey aspires to develop and grow an innovation economy, in which entrepreneurship and innovation are crucial components for long term economic prosperity and societal gains, it must also create a cyber ecosystem that develops a trustworthy environment and helps to manage cybersecurity risks.



THREAT ENVIRONMENT

Cybersecurity attacks made headlines and garnered the public's attention as a result of large scale and increasingly frequent data breaches beginning with the breach of Target in 2013 that resulted in the compromise of over 40 million Target customers' payment card data. Since that time, numerous public and private sector organizations have fallen victim to data breaches in which financial account information, Social Security numbers, health records, and other sensitive personally identifiable information of millions of individuals were stolen. And while these attacks are most relatable to the individuals - the general public - whom they impact, even more nefarious cyberattacks have targeted physical systems, threatening lifeline critical infrastructure sectors including electricity, water, transportation, and communications.



Cyberattacks are increasing, both in prevalence and disruptive potential. Since 2019, over 1,500 cybersecurity incidents were reported to the NJCCIC by impacted individuals and organizations. Among the most damaging to NJ institutions in both costs and debilitating operational impacts were the more than 120 reported ransomware attacks, with victims including police departments, municipal and county governments, school systems, health care organizations, utilities, and private businesses. Reporting cybersecurity incidents to the NJCCIC is voluntary for most organizations. As such, it is estimated that the true number of incidents is much greater than the numbers reported.

Cyberattacks are not constrained by geographic boundaries; attacks launched against systems in geographies outside New Jersey may have collateral effects that threaten and/or impact individuals and institutions in the State. Conversely, cyberattacks launched against networks and systems in New Jersey may have cascading effects across the region, the nation, and the world. The capability to carry out crippling attacks is not solely the domain of nation state actors. Individual criminals and criminal syndicates, hacktivists, terrorist groups, and other threat actors can carry out destructive and costly attacks for a host of motivations. Such attacks ultimately lead to the loss of critical information and information systems that threaten public safety, undermine public confidence, have a negative effect on the economy and diminish the security posture of the State of New Jersey and, more broadly, the United States.

Whether you're an individual or a public or private sector organization, you are not immune to cyberattacks. On a monthly basis, the NJCCIC detects and blocks over 10 million attacks targeting New Jersey State Government networks, systems, and users. Anything and anyone connected to the Internet can be a target. As with physical defenses, it is unrealistic to think that even the most steadfast cyber defenses are impenetrable. Recognizing this, the NJCCIC strategic plan not only incorporates cyber prevention goals and objectives intended to mitigate the risks and impacts of cyberattacks, but also includes equal focus on building capabilities necessary to detect, respond to, and recover from them, thereby making New Jersey more resilient to the inevitability of successful cyberattacks.

> *"It's clear where the world is going. We're entering a world where every thermostat, every electrical heater, every air conditioner, every power plant, every medical device, every hospital, every traffic light, every automobile will be connected to the Internet. Think about what it will mean for the world when those devices are the subject of attack." Then he made his pitch. "The world needs a new, digital Geneva Convention."*
>
> — Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

THE THREAT ENVIRONMENT
TIMELINE OF NOTABLE GLOBAL CYBERSECURITY INCIDENTS

- In 2013, Iranian hackers associated with the Islamic Revolutionary Guard infiltrated the controls of a small dam located approximately 20 miles north of New York City.
- In December of 2015, Russian state-sponsored hackers launched cyberattacks against the Ukraine power grid causing the first cyber-induced blackouts that affected hundreds of thousands of homes and businesses.
- In June of 2016, Russian hackers infiltrated the online voter registration systems of the states of Illinois and Arizona, and carried out other cyber and influence operations in attempts to impact the integrity of the election processes in the United States.
- Also in 2016, the largest ever distributed denial-of-service attack involving thousands of Internet of Things devices was launched against Domain Services Provider Dyn DNS, resulting in an outage that affected approximately 1/3 of the internet. Notably, the malicious code that was used to carry out this attack was created by a NJ resident, Paras Jha, who was subsequently arrested and prosecuted.
- In 2017, two of the most destructive cyberattacks affected systems worldwide. The May 2017 Wannacry ransomware attack that has since been attributed to North Korean state sponsored hackers impacted approximately 300,000 computers across 150 countries, including in the UK where hospitals and clinics were forced to turn away patients and cancel operations.
- Then in June, NotPetya, the most destructive cyberattack in history impacted thousands of organizations worldwide causing over $10 billion in losses and damages. New Jersey-based Merck Pharmaceuticals was one of the victim organizations, which not only cost Merck hundreds of millions in financial damages but also impacted its ability to produce critical vaccines. Another NotPetya victim, Maersk, saw its ability to conduct shipping operations crippled and caused the shutdown of the Port of Newark. Losses and damages related to NotPetya for just Merck and Maersk are estimated at $1.2 billion. NotPetya has since been attributed to Russian state-sponsored hackers.
- In March of 2018, the US Department of Justice indicted nine Iranian hackers alleged to have carried out attacks against more than 300 universities in the United States and abroad.
- In November 2018, Starwood Hotels confirmed its hotel guest database of about 500 million customers had been stolen in a data breach. The hotel and resorts giant said in a statement filed with US regulators that the “unauthorized access” to its guest database was detected on or before September 10, 2018 — but may date back as far as 2014.
- In 2019, a cloud database configuration vulnerability was exploited, resulting in the breach of over 100 million Capital One customers.
- In 2020, cyber criminals and nation states have acted to exploit the COVID-19 pandemic through various cyber scams and frauds for financial gain, and intrusions targeting intellectual property related to response strategies, and potential vaccines and treatments research.

NEW JERSEY'S APPROACH TO CYBERSECURITY

The mission of the New Jersey Office of Homeland Security and Preparedness is to lead and coordinate New Jersey's counterterrorism, cybersecurity, and preparedness efforts.

Executive Order No. 5 signed by Governor Corzine on March 16, 2006, established the New Jersey Office of Homeland Security and Preparedness (NJOHSP) as the State Agency responsible for administering, coordinating, leading, and supervising New Jersey's counter terrorism, and preparedness efforts. NJOHSP is led by a Director, who also acts as the State's Homeland Security Advisor and the Chair of the Domestic Security Preparedness Task Force, which in accordance with the New Jersey Domestic Security Preparedness Act P.L. 2001 c.246, is responsible for effectuating the coordination of the disaster preparedness and recovery resources, as well as the management, coordination, administration of responses to any terrorist attack or any other technological disaster.

As a result of Executive Order No. 178, signed by Governor Christie on May 20, 2015, the NJOHSP, through a newly formed component organization, the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), was tasked with leading and coordinating New Jersey's cybersecurity efforts while building resiliency to cyber threats throughout the State. By organizing cybersecurity under the NJOHSP, the State centralized responsibility and accountability for statewide cybersecurity efforts, beyond just those of New Jersey State Government networks, systems, and information. Located at New Jersey's Regional Operations and Intelligence Center (ROIC) and, acting in a combined cyber fusion and security operations center capacity, the NJCCIC is staffed by personnel from the NJOHSP, the New Jersey Office of Information Technology (NJOIT), and the New Jersey State Police (NJSP), thereby providing a multi-agency and multi-disciplinary "all threats/all hazards" approach to cybersecurity.

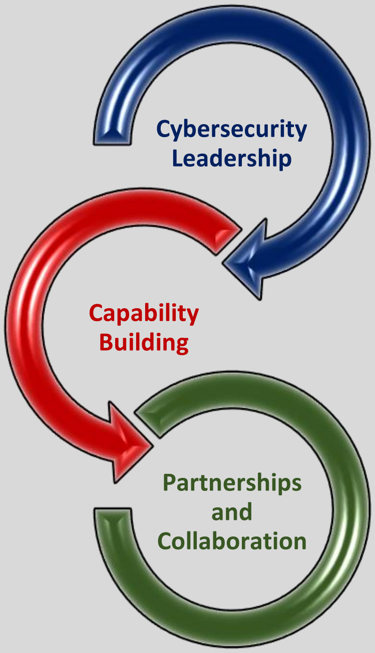
In addition to the three primary agencies that comprise the NJCCIC, partnerships with a number of other key stakeholders have been developed, including but not limited to, the New Jersey Office of the Attorney General, the New Jersey National Guard, the New Jersey Board of Public Utilities, the Federal Bureau of Investigation, the US Department of Homeland Security; national information security organizations such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), Health Information Sharing and Analysis (H-ISAC), Financial Services Information Sharing and Analysis Center (FS-ISAC), and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC); as well as public and private sector organizations and operators of critical infrastructure and key resources throughout New Jersey and beyond. These partnerships ensure critical information is shared broadly and key resources are coordinated across applicable sectors in a whole-of-state approach to cybersecurity in New Jersey. At the same time, the NJCCIC realizes that, while its focus is on making New Jersey more resilient to cyberattacks, it also has a role to play in making the region, the nation, and the world more resilient.

> *"Cyber security is an information technology issue, but not only an information technology issue. It is a law enforcement issue, but not only a law enforcement issue. It is a national and homeland security issue, but not only those things. New Jersey, by combining the three in its approach to dealing with cyber security seems to be offering up an important model – "the Garden State model" - of how the sad state of cyber security can begin to get better, and how states can contribute to that improvement."*
>
> *- The Center for Information Security*
> *at Stanford Law School*

STRATEGIC PLAN GOALS, OBJECTIVES, AND ACTION ITEMS

This strategic plan represents a pathway to achieving improved cyber resilience through the prosecution of a series of interrelated goals, objectives, and action items intended to help safeguard New Jersey's institutions, businesses, and individuals. It includes broad statewide goals and objectives applicable to all public and private sector institutions and individuals, as well as those specific to the executive branch of New Jersey State Government, for which the NJCCIC has direct oversight. This strategic plan also supports the overall mission of the New Jersey Office of Homeland Security and Preparedness, whereby cybersecurity is woven into its counterterrorism, counterintelligence, and preparedness functions.

NJCCIC STRATEGIC GOALS



Cybersecurity Leadership: Lead and coordinate a whole-of-state approach to cybersecurity.

Capability Building: Increase the resilience of public and private institutions, critical infrastructure assets and key resources, and the citizens of New Jersey.

Partnerships and Collaboration: Cultivate strategic partnerships and pervasively collaborate with public and private sector organizations.

STRATEGIC GOAL 1: CYBERSECURITY LEADERSHIP

Lead and coordinate a whole-of-state approach to cybersecurity.

In 2015, the NJCCIC was established as a component organization within the NJ Office of Homeland Security and Preparedness and was tasked with the responsibility of serving as the central civilian resource for cybersecurity leadership and coordination for a broad range of statewide cybersecurity initiatives and efforts. Since its inception, the NJCCIC has delivered significant public benefit and value in protecting New Jersey's institutions, businesses, and individuals against a growing number of cyber threats. Strategic Goal 1 builds upon those successes and addresses the NJCCIC’s role in leading and coordinating a whole-of-state approach to cybersecurity.

OBJECTIVE 1.1: Establish and grow the NJCCIC as a Cybersecurity Center of Excellence (CCOE) that provides leadership, best practices, training, support, and research.

Action Items:

- Provide thought leadership and champion the adoption of cybersecurity best practices and initiatives across New Jersey in the face of new and emerging cybersecurity risks and threats.

- Establish an NJCCIC Cybersecurity Advisory Committee consisting of cybersecurity leaders and subject matter experts from industry, government and non-government organizations, and academia to help provide direction and support for whole-of-state cybersecurity efforts.

- Research, develop, support, and implement innovative processes, practices, and technologies in order to improve the efficiency and effectiveness of New Jersey's cybersecurity efforts.

- Update and align New Jersey's cybersecurity strategy to meet evolving threats and societal needs.

- Take an active role in leading and influencing national cybersecurity initiatives.

- Develop strategies and tactics necessary to address threats introduced by the continued digital transformation of work and society (e.g. IoT, 5G, smart cities, artificial Intelligence, autonomous vehicles, etc.).

- Support and participate, where appropriate, in private sector and academic cybersecurity research and development initiatives.

- Identify and attain grant funding to support the development and implementation of innovative cybersecurity programs of work, practices, and technologies.

OBJECTIVE 1.2: Champion and grow a culture of cybersecurity and privacy across executive branch departments and agencies.

Action Items:

- Develop, adopt, and institute cybersecurity best practices, standards, and frameworks across executive branch departments and agencies.

- Institute a continuous improvement program that measures, assesses, and implements policies, processes, standards, and technologies necessary to establish sufficient assurance levels are maintained for systems and program maturity.

- Ensure cybersecurity investments are risk-based and provide prioritized protections for New Jersey's most critical and sensitive assets.

OBJECTIVE 1.3: Promote and implement cybersecurity education and training initiatives.

Action Items:

- Continue collaboration with NJ Department of Education on the development of a statewide computer science curriculum that integrates cybersecurity education.

- Partner with K-12 and higher education institutions to develop cybersecurity education and training programs.

- Continue to coordinate and grow participation in hands-on educational opportunities for K-12 and higher education students, including programs, such as Girls Go CyberStart program, Cyber Patriot, Capture the Flag, etc.

- Grow and support cybersecurity internship, apprenticeship, and scholarship for service programs necessary to develop a capable cyber workforce.

- Support and implement cybersecurity training and education initiatives for professional development and reskilling current workers.

OBJECTIVE 1.4: Advocate for and support legislative efforts and government initiatives that improve cybersecurity posture of the State.

Action Items:

- Provide reports to legislative committees on cybersecurity threats, risk posture, and best practices.

- Monitor, review, and provide input on legislation that includes a cybersecurity nexus.

- Support legislative and regulatory activity that promotes cybersecurity and data privacy protections.

- Provide input and support for efforts to consolidate accountability for harmonizing the cybersecurity policies, budgets, and responsibilities necessary to achieve uniformity and the overall improvement of the cybersecurity postures of executive branch departments and agencies.

- Support efforts to create cybersecurity jobs and expand the cybersecurity industry in New Jersey.

- Lead and support efforts to improve inefficient state government business processes and unnecessary bureaucratic structures that introduce unnecessary risk and act as obstacles to achieving cyber resilience.

OBJECTIVE 1.5: Measure, assess, and drive improvements to the New Jersey's cybersecurity posture.

Action Items:

- Expand implementation of intelligence-driven cybersecurity efforts.
- Prioritize cybersecurity investments based on risk.
- Collect, process, and analyze security telemetry and threat data to aid in identifying emerging threats, trends, and risk management strategies.
- Develop dashboards and produce cybersecurity progress reports to key stakeholders that identify trends, risks, emerging threats, and key performance indicators.

STRATEGIC GOAL 2: CAPABILITY BUILDING

Increase the security posture and resilience of public and private institutions, critical infrastructure assets and key resources, and the citizens of New Jersey by building cybersecurity capabilities.

Resilience, as defined by Presidential Policy Directive PPD-21, is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience focuses on the preventive, detective, and reactive controls in an information technology environment to assess gaps and drive enhancements to improve the overall security posture of the entity. This strategic goal addresses the State's cybersecurity readiness and cyber resilience, including those initiatives and activities necessary to prepare for, respond to, and recover from cyberattacks.

OBJECTIVE 2.1: Develop and implement a cybersecurity risk management program.

Action Items:

- Build the necessary structures and processes to assess and manage cyber risk across New Jersey.
- Update, as appropriate, the Statewide Information Security Manual that prescribes a risk–based approach to information security while establishing the required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals.
- Develop and grow the capability to conduct cybersecurity surveys and assessments of public and private sector cybersecurity programs and systems.
- Develop and implement a supply chain security program that establishes baseline requirements and institutes a vendor assessment platform through which security due diligence assessments are standardized and shared with relevant stakeholders.

- Develop a security assessment function that ensures the security and privacy controls for major systems and applications, and general support systems in the executive branch of New Jersey State Government are assessed, and risks are managed to acceptable levels, prior to deployment to operational status.

- Continually test executive branch networks, systems, and applications to identify vulnerabilities, gaps in cyber defenses, and emerging threats.

- Engage independent third parties to review and assess the appropriateness of the cybersecurity program and the controls that safeguard executive branch systems.

OBJECTIVE 2.2: Fortify New Jersey's cyber defenses.

Action Items:

- Provide direct and indirect support to executive branch and other public and private sector organizations in implementing cybersecurity best practices and technologies.

- Expand the breadth, capability, and effectiveness of the NJCCIC's managed security services.

- Research, identify, acquire, deploy, and monitor effective preventive and detective security technologies and services.

- Establish uniformity of cybersecurity controls, technologies, and processes across executive branch departments and agencies.

- Partner with the NJ Office of Information Technology and other executive branch departments and agencies to develop a technology roadmap that incorporates security and privacy by design.

- Lead and support efforts to modernize and harden New Jersey's technology infrastructure.

- Increase the security posture (people, process, technology) for a remote workforce environment.

- Leverage data analytics to identify threats and implement controls to safeguard against them.

OBJECTIVE 2.3: Increase the capacity to respond to and recover from significant cyber incidents.

Action Items:

- Continue to develop the NJCCIC Security Operation Center's monitoring, alerting, and response capabilities to identify and effectively respond to cybersecurity incidents.

- Develop and publish an incident response plan to include a defined methodology and individual playbooks necessary to ensure a consistent and organized response to incidents.

- Develop and implement tools, technologies, and practices for use in handling cybersecurity incidents.

- Develop, conduct, and participate in cybersecurity incident response exercises internally with executive branch departments, and externally with public and private sector organizations.

- Enhance coordination of cybersecurity incident handling among federal, state, and local partners, including emergency management teams and operators of critical infrastructure and key resources.

- Develop NJCCIC capabilities that augment an impacted organization's capabilities to respond to and recover from a cybersecurity incident.

- Establish a New Jersey Cyber Corps comprised of public and private sector resources that can provide assistance in response to and recovery from significant cybersecurity incidents.

- Periodically review the Cybersecurity Annex to the State Emergency Operations Plan for appropriateness and relevance, and update as necessary.

OBJECTIVE 2.4: Establish a cyber talent management program that attracts, develops, and retains highly skilled and capable cybersecurity professionals.

Action Items:

- In partnership with the Civil Service Commission, develop cybersecurity titles and career tracks to meet current and future needs of state and local governments in attracting and retaining capable cybersecurity professionals.

- Provide executive branch cybersecurity personnel with resources and opportunities to continually improve and develop knowledge, skills, and abilities required to address evolving cybersecurity challenges and to enable career advancement opportunities.

- Further develop and expand the NJCCIC's internship, apprenticeship, and scholarship opportunities.

OBJECTIVE 2.5: Lead and support efforts that increase the capability and capacity of all New Jerseyans to recognize and mitigate cyber risks.

Action Items:

- Develop, implement, and deliver online and in-person cybersecurity training offerings for public and private sector organizations, individual citizens, and community organizations.

- Develop and distribute relevant security awareness materials, alerts, and advisories, and provide notifications to key stakeholders of new and/or updated statutes, regulatory requirements, and policies.

- Implement a virtual cyber range to provide hands-on cybersecurity and incident handling training to government and non-government entities and individuals.

- Conduct regular cybersecurity exercises to test and improve the ability of executive branch employees to identify and mitigate risks.

OBJECTIVE 2.6: Protect New Jersey elections from cyber threats and influence operations.

Action Items:

- In partnership with the NJ Secretary of State's Office, provide cybersecurity support in securing state and local elections systems.

- Develop a taskforce and coordinate elections security efforts across state, federal, local, and non-government partner organizations.

- Champion and drive cybersecurity best practices, standards, frameworks, and technologies across the elections ecosystem in New Jersey.

- Establish continuous monitoring, alerting, and incident response capabilities specific to elections infrastructure.

- Engage industry partners to help implement solutions that bolster the security of New Jersey's elections infrastructure.

STRATEGIC GOAL 3: PARTNERSHIPS AND COLLABORATION

Cultivate strategic partnerships and pervasively collaborate with public and private sector organizations to increase the capacity and capability to recognize threats, defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of New Jersey and the United States.

Strategic Goal 3 recognizes that, in a hyper-connected world, all organizations face a common set of threats for which a collaborative, whole-of-state approach allows for the sharing of critical information and key resources, and the integration of public and private sector cyber defense and response capabilities. The principle of *One Team/One Fight* whereby many different organizations and individuals come together for a common mission is a key component of this strategic goal.

> *"One example I'd look at is the New Jersey Cybersecurity & Communications Integration Center, the NJCCIC. And what they've done is outreach to critical infrastructure partners in the state that include private sector partners."*
>
> -Timothy Blute, Program Director, NGA Center for Best Practices,
> Homeland Security & Public Safety Division

OBJECTIVE 3.1: Develop new and strengthen current partnerships.

Action Items:

- Establish strong and improved engagement programs and trusted partnerships with public and private sector organizations, Information Sharing Analysis Centers and Organizations (ISACs and ISAOs), and other non-government cybersecurity organizations.

- Strengthen and grow the partnerships with federal, state, local and NJ National Guard partners to increase the capacity and capability to defend against and respond to cyberattacks perpetrated against the citizens, public and private institutions, and the critical infrastructure of New Jersey and the United States.

- Integrate and improve public and private-sector cyber defense and response efforts.

- Increase federal and state grant funding utilization to help bolster the cybersecurity posture of critical infrastructure and key resources across New Jersey.

- Improve incorporation of the NJCCIC's programs of work with those of the NJOHSP's counterterrorism, counterintelligence, and preparedness functions.

- Bolster the NJCCIC's role and effectiveness within the NJ Regional Operations and Intelligence Center and expand its engagement with fusion centers throughout the United States.

- Improve coordination of the NJCCIC's statewide cybersecurity efforts with New Jersey Urban Area Security Initiative (UASI) Program representatives to ensure high-threat, high-density urban areas have the appropriate resources to prevent, protect against, mitigate, respond to, and recover from cyberattacks.

- Establish new and grow current partnerships with academia, including K-12, higher education, and private sector educational organizations, to ensure development of required cybersecurity knowledge, skills, and abilities.

OBJECTIVE 3.2: Strengthen the NJCCIC's ability and effectiveness in collecting, analyzing, and disseminating cyber or other relevant information in order to enable potential targets to recognize threats and defend and respond more effectively, reducing the likelihood that those attacks and attackers will succeed.

Action Items:

- Observe, gather, and analyze critical cyber and related information in order to better understand security problems and inter-dependencies related to cyber systems, so as to ensure their confidentiality, integrity, and availability.

- Disseminate relevant and timely cyber and related information to NJCCIC members; federal, state and local governments; and other entities that may be of assistance in preventing, detecting, mitigating, or recovering from the effects of a cyberattack.

- Continue to add relevant cybersecurity content and features to NJCCIC web and social media properties.

- Develop an interactive web portal for cybersecurity communications and information sharing with NJCCIC members.

- Deploy a bi-directional threat intelligence platform for use by public and private sector organizations.

- Author, collaborate on, and publish research papers and articles in trade journals and other relevant publications.

- Expand delivery platforms to include live and recorded audio and video content.

OBJECTIVE 3.3: Communicate and share critical cyber and other relevant information by hosting, coordinating, and participating in cybersecurity symposiums, conferences, workshops, briefings, and events.

Action Items:

- Coordinate and host an annual Statewide Cybersecurity Conference.

- Develop and conduct sector- and audience-specific cyber symposiums, threat briefings, presentations, and workshops.

- Participate as cybersecurity subject matter experts for industry and government conferences and events.

- Develop, host, and participate in online webinars, presentations, and trainings.

CRITICAL SUCCESS FACTORS

The successful execution of this strategic plan will broadly depend on or be influenced by the following considerations.

Management Endorsement - It is essential that this strategic plan is endorsed and driven at the highest levels of the executive branch of New Jersey State Government and that it receives the full support of the Director and Deputy Director of the New Jersey Office of Homeland Security and Preparedness, and the Domestic Security Preparedness Task Force. The Director of the Office of Homeland Security and Preparedness should identify and establish State cybersecurity priorities and provide budgetary and human resources needed to implement the strategy.

Resource Prioritization - As the threat landscape is both evolving and expanding, it is critical to continuously advance New Jersey's security, resilience and operational capacities. The prioritization and fluid allocation of key resources is necessary to maintain currency and effectively protect against and respond to significant cybersecurity incidents.

Shared Responsibility - Cybersecurity is a shared responsibility beyond New Jersey State Government alone. As cyberspace consists of a hyper-connected array of networks, systems, and devices, the cooperation of all key stakeholders – government, industry, non-government organizations, and academia – is essential to not only the success of this strategic plan, but also the public health, welfare, and safety of the citizens, economy, and public interests of the State of New Jersey and national security.

Human Capital - As cybersecurity is a highly technical and complex discipline that requires qualified and skilled human resources at sufficient staffing levels, the ability of the NJCCIC to recruit, develop, and retain talented and mission-focused personnel is critical to carrying out this strategic plan.

Funding - This strategic plan was drafted assuming that funding levels for cybersecurity would remain stable and additional investments would be made over time to address the growing threat environment and to protect the public and private institutions, critical infrastructure assets, and the citizens of New Jersey from the threat of cyberattacks.

AUTHORITIES

New Jersey Domestic Security Preparedness Act P.L. 2001, c.246 establishes a New Jersey Domestic Security Preparedness Task Force that includes the New Jersey Office of Homeland Security and Preparedness, the New Jersey National Guard, the Office of Emergency Management in the Division of State Police, among other state, county, and local organizations in order to maximize, enhance, and effectuate coordination of the disaster preparedness and recovery resources. Included in the duties of the task force is the development, implementation, and management of comprehensive responses to any terrorist attack or any other technological disaster and the effective administration, management, and coordination of remediation and recovery actions and responses following any such attack or disaster.

State of New Jersey Executive Order No. 5 signed by Governor Corzine on March 16, 2006 establishes the New Jersey Office of Homeland Security and Preparedness as the State Agency responsible for administering, coordinating, leading, and supervising New Jersey's counterterrorism and preparedness efforts. NJOHSP is led by a Director, who also acts as the State’s Homeland Security Advisor and the Chair of the Domestic Security Preparedness Task Force. The Director and the NJOHSP shall be authorized to call upon the expertise and assistance of all State departments, divisions, and agencies to carry out their mission. The NJOHSP may, to the extent not inconsistent with any other law, employ, consult, and contract with private and public entities, and enter into such agreements with public and private individuals or entities as necessary to further the mission of the Office or of other offices and units that fall under the Director's supervision.

State of New Jersey Executive Order No. 178 signed by Governor Christie on May 20, 2015 establishes the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) as a component organization within the Office of Homeland Security and Preparedness that acts as the central State civilian interface authorized to coordinate cybersecurity information sharing and analysis across all levels of government, agencies, authorities, and the private sector pursuant to 6 U.S.C. § 133 et seq. The NJCCIC is authorized to draw upon the assistance of any department, office, division, or agency of this State to supply it with expertise and assistance, including information and personnel, to carry out the NJCCIC mission. The NJCCIC is composed of representatives of State entities, including the Office of Homeland Security and Preparedness, the Division of State Police, and the Office of Information Technology.

State of New Jersey Technology Circular 17-00-NJOIT, October 14, 2017, establishes a management structure for information security across the executive branch of New Jersey State Government including the roles and responsibilities of the Director of the Office of Homeland Security and Preparedness, the State Chief Technology Officer, the State Chief Information Security Officer, and the Director of the New Jersey Cybersecurity & Communications Integration Cell.